Privileged User Governance—A Key to Effective Breach Protection

Privileged Accounts—Why Do We Care?

As we’ve seen from many of the headlines lately, breaches continue to do extensive financial and reputational damage to many major companies. A recent analyst report indicates that the average breach costs the organization $4 million in total costs, which represents $158 per breached user record. Other studies have consistently shown that the root cause of most breaches is stolen privileged user credentials.

With the prevalence of these attacks, the need for controlling access to privileged accounts has increased in importance. But simply controlling what a privileged user can do isn’t enough. Even organizations that have effective privileged access management solutions in place face challenges in governing privileged user access on a continuous basis. In addition, separate mechanisms for governance of regular and privileged users introduce risk, increase management complexity and reduce the organization’s visibility into the full identity context. What organizations need is a unified approach to access governance across all users.

The Privileged User Management Lifecycle

Managing privileged users is a continuous and critical process. First, you must discover where your admin accounts are and eliminate improper privileges and orphan accounts. Next, you must enforce your least-privilege policies for these users and eliminate shared accounts—this is called privileged access management (PAM). Lastly, you must govern privileged access to avoid entitlement creep and to ensure that each user still needs any elevated privileges that they have. If any one of these essential capabilities are weak or missing, your overall risk of breach or insider threat rises significantly.
In the CA Security portfolio, enforcement is done with CA Privileged Access Manager; discovery/governance is provided by CA Identity Suite.

**Privileged user governance** is the process of ensuring that all users of privileged accounts gain and maintain the appropriate level of access to those accounts and credentials. This has become much more challenging recently because application deployment is more diverse (on-premises, cloud), and because user relationships are more dynamic with partners and contractors coming and going frequently on a temporary basis. But, privileged user governance is a critical capability because your auditors will ask you for proof that each user of a privileged account is properly authorized; without effective governance, you will not pass that audit.

Many organizations have processes in place for governing regular user access, but have no method (or a different method) for governing privileged access. This results in a security silo that increases the risk of excessive entitlements, especially among privileged users. The benefits of integrating a PAM solution and governance platform include:

- A single point of control for managing identities across all users
- Simplified on-/off-boarding of all users across the extended enterprise
- Improved visibility into privileged access across all users
- Reduced risk of excessive entitlements or segregation of duties (SoD) violations
- Common processes for access request/approval/certification for all users
Key capabilities for privileged user governance

To reduce risk, privileged users should be granted access based on the principle of least privilege, that is, the minimal access needed to perform their job function. There are four phases within the lifecycle of a privileged user that are relevant for governance—when they are initially provisioned, when they request additional access, when their access is certified and when they are deprovisioned. All are important control points in order to ensure that least privilege is enforced.

- **Access provisioning/deprovisioning.** Provisioning should be automated with flexible approval workflows and should allow temporary access for specific individuals. Immediate deprovisioning is critical because often, the departing privileged user may now have a grudge against the company. Also, time-limited entitlements need to be removed to avoid proliferation of privileged credentials.

- **Access requests.** This is when appropriate checks are put in place to validate that this user actually requires access to a sensitive account, and that the request doesn’t violate any established security policies.

- **Access certification.** Managers need to certify the entitlements of their employees. But simply automating the process is not sufficient. Information needs to be provided to the certifier to help them make a more-informed decision about whether each user’s access is still valid. Contextual information about the user and their access is what brings important insight to the certification process.

Integrating CA Identity Suite with CA Privileged Access Manager (CA PAM) provides automated provisioning and deprovisioning of access to privileged accounts, along with role and group management of all privileged users. The deep integration enables more granular control over privileged roles, groups, start/stop dates and other attributes of privileged users. Privileged access can be provisioned on a time-limited basis, so that temporary credentials can be granted but automatically removed at a specific date and time.

The process of requesting privileged access is a common occurrence. To improve productivity, the user experience (for both requester and approver) must be simple and convenient. More important, access that violates security policy, for example, a segregation of duties (SoD) violation, must be prevented automatically without relying on the approver to recognize these violations.

CA Identity Suite provides a unique approach to governance that helps ensure that least privilege is enforced, while providing a rich, yet easy-to-use experience for both requesters and approvers. This approach lowers risk through three key capabilities:

- **Business Entitlements Catalog.** All entitlements and systems can be mapped from IT-centric names to business terms the user can more easily recognize to help greatly simplify requests, approvals and certifications.
• SoD checks. All requests are checked automatically for compliance with SoD policies. This is particularly critical for privileged users because their level of access is already very high, so improper combinations of entitlements need to be prevented.

• Context-based risk analysis. Sometimes, a request for access poses more-than-normal risk, even for a privileged user. Case in point: as a user accumulates access to several privileged accounts, their risk of each such access increases because this person eventually may have more access than they absolutely require. CA Identity Suite calculates a risk score for each access request based on a number of factors, such as the sensitivity of the resource, the user’s role, whether others in the same role have that access, etc. The approver can evaluate this risk level and the reasons for it to make a more-informed decision. The following graphic highlights this process flow for the access request process.

Though risk management is the primary driver behind the increased emphasis on privileged user control and governance, the quality of the user experience is critical. CA Identity Suite provides a simple, intuitive and business-oriented user experience that streamlines the entire access request process. Access is requested through a familiar shopping-cart model and complex IT terms are mapped to more familiar terms through the Business Entitlements Catalog. The interface can also be localized so that the requestor and approver can work in their own native languages. These capabilities help increase productivity and satisfaction, while lowering the overall risk of improper privileged entitlements.
Access Certification—Eliminating Unnecessary Entitlements

Access certification is an essential step in effective governance of all users, but especially for privileged account users. Enterprises need a convenient, simple way to ensure that all access to privileged accounts is periodically (and frequently) certified as still being required.

There are often two challenges to this process that existing solutions don’t meet:

- Certification fatigue. Managers might have to certify so many people that they opt for mass approvals without paying adequate attention to the access requirements of each individual user.
- Inadequate contextual information. Managers might be asked only to certify access for a user, but no additional information about the relative risk of this access is provided. The result? A poor, uninformed certification decision.

CA Identity Suite solves the first problem by providing a rich, but easy-to-use, customizable user experience. Information about each user and their access can be presented and grouped according to the preferences of each certifier. In addition, CA Identity Suite can show information about the previous certification campaign actions, which helps streamline the entire process—especially if few changes are expected.

In short, access certification becomes far less of a chore; instead, it’s a simple operation that can be done easily, which reduces risk.

The solution also provides risk-based contextual information, which helps managers focus their attention on the risk level of each user’s access. For example, a particularly risky access privilege is highlighted to the certifier so that inadvertent certification errors can be dramatically reduced.

Access certification is at the heart of effective privileged user governance, but it doesn’t need to be the painful, time-consuming process that it often is. An intuitive, business-focused user experience can help streamline this process, improve user satisfaction and eliminate careless certification errors.

Figure A.
The screen shot highlights the use of risk scoring during the approval process. In this case, the user already has a risk level of 400 based on the access rights that they already have. The new, requested access brings that risk score up to 550, possibly based on the sensitivity of the resource, or other factors relating to this requester. In this case, the approver can easily understand the risk level of this request, and can accept, reject, or delegate this request according to establish security policy. The result is a much higher quality access decision, and lower risk.
Benefits of Privileged Identity Governance

CA Identity Suite is integrated with CA Privileged Access Manager to provide provisioning, deprovisioning and governance of access to privileged accounts across the enterprise. These capabilities provide several very important benefits to help organizations:

**Improve security.** The solution provides visibility to help identify and correct improper or redundant access to privileged users, and enforces SoD policies, enabling managers to quickly and easily analyze and certify the access of each of their privileged users.

**Simplify compliance:** Governing privileged access is a major element of many regulations, so an effective solution is essential for successful audits. Mandates such as ISO 27002 (sections 8.1.2, 9.2.5), the Payment Card Industry Data Security Standard (PCI DSS) and others specifically include requirements for privileged access governance.

**Eliminate silos:** Implementing separate governance solutions for privileged access and non-privileged access may create unintended weaknesses in your cyber-security strategy. A single governance approach promotes consistency and reduces risk.

For more information, please read the e-book, “Managing and Governing Identities in the New Open Enterprise.”

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.


© Copyright 2016 CA. All Rights Reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.